Claims

WHAT IS CLAIMED IS:

1. A method for policy and attribute based access to a resource, comprising:

interacting with a principal for authenticating the principal based on acquired identity information;

assembling an identity configuration for the principal;

generating a service contract for the principal, a service, and a resource, wherein the principal uses the service to access the resource, and wherein the service contract includes a selective number of resource access policies and attributes which are included in the identity configuration; and

transmitting an access statement to the principal for use when the principal interacts with the service.

2. The method of claim 1 further comprising generating alias identity information for the identity information and including the alias identity information with at least a portion of the access statement.

3. The method of claim 2 further comprising:

receiving the alias identity information from the service;

mapping the alias identity information back to the identity information;

authenticating the identity information; and

permitting the service to the resource based on the service contract.

4. The method of claim 1 wherein the transmitting of the access statement further includes representing the access statement as an assertion that is directly used to acquire the identity information of the principal.

5. The method of claim 1 wherein the transmitting of the access statement further includes representing the identity information of the principal as an artifact

that can be indirectly used to acquire the identity information.

6. The method of claim 1 further comprising removing the service contract when an active session with the principal expires.

7. The method of claim 1 wherein the interacting further includes establishing a secure communication with the principal.

8. A method for policy and attribute based access to a resource, comprising:

receiving a session request for access to a resource, wherein the session request is sent from a service and includes alias identity information for a principal;

mapping the alias identity information to identity information of the principal;

authenticating the identity information;

acquiring a service contract for the principal, the service, and the resource, wherein the service contract includes selective resource access policies and attributes which are permissibly used by the service on behalf of the principal; and

establishing a session with the service, wherein the session is controlled by the service contract.

9. The method of claim 8 further comprising accessing an identity configuration for the principal in order to acquire the selective resource access policies and attributes included within the service contract.

10. The method of claim 8 further comprising denying access attempts made by the service during the session when the access attempts are not included within the service contract.

11. The method of claim 8 further comprising terminating the session when an event is detected that indicates the service contract is compromised or has expired.

12. The method of claim 8 further comprising establishing the service contract with the principal prior to receiving the session request.

13. The method of claim 12 further comprising reusing the service contract to establish one or more additional sessions with the service, wherein the one or more additional sessions are associated with one or more additional session requests made by the service.

14. The method of claim 12 wherein the establishing further includes establishing the service contract with the principal in response to a redirection operation performed by a proxy that intercepts a browser request issued from the principal to the service for purposes of accessing the resource.

15. A policy and attribute based resource access system, comprising:

an identity authenticator;

an identity configuration aggregator; and

a resource session administrator;

wherein the identity authenticator authenticates a principal for access to a resource based and generates a service contract, and wherein the identity configuration aggregator generates an identity configuration for the principal and the resource, the service contract defines selective resource access policies and attributes from the identity configuration, and wherein the resource session administrator establishes a session with a service and ensures that access attempts made by the service during the session conform to the service contract.

16. The policy and attribute based resource access system of claim 15 wherein the system is implemented as a proxy server.

17. The policy and attribute based resource access system of claim 15 wherein the service contract is generated in response to an intercepted resource-access request made by the principal to the service.

18. The policy and attribute based resource access system of claim 17, wherein the resource-access request is redirected by a Hyper Text Transfer Protocol (HTTP) Proxy serving as an intermediary between the principal and the service.

19. The policy and attribute based resource access system of claim 15, wherein the service contract is generated in response to a redirected resource-access request made by the principal to the service, and wherein the service redirects the resource-access request to the system.

20. The policy and attribute based resource access system of claim 15, wherein the service contract expires when an active session with the principal expires.

21. A policy and attribute based resource session manager, residing in a computer-accessible medium, comprising instructions for establishing a session with a resource, the instructions when executed performing the method of:

receiving alias identity information from a service, wherein the alias identity information is associated with a principal;

requesting a mapping of the alias identity information to principal identity information;

requesting authenticating of the identity information;

requesting a service contract for the principal, the service and a resource, wherein the service contract includes selective resource access policies and attributes derived from an identity configuration; and

establishing a session with the service and the resource, wherein the session is controlled by the service contract.

22. The policy and attribute based resource session manager of claim 21 having instructions further comprising, permitting the service to indirectly access an identity store which represents the resource, and wherein the identity store includes secure information related to the principal.

23. The policy and attribute based resource session manager of claim 21 having instructions further comprising terminating the session when the service contract expires or is compromised.

24. The policy and attribute based resource session manager of claim 21, wherein the requesting of the mapping further includes interacting with an alias translator.

25. The policy and attribute based resource session manager of claim 21, wherein the requesting of authentication further includes interacting with an identification authenticator.

26. The policy and attribute based resource session manager of claim 21 having instructions further comprising managing the session by acting as an intermediary between the service and a legacy Lightweight Directory Access Protocol (LDAP) application which has access privileges to the resource.

27. The policy and attribute based resource session manager of claim 26, wherein the receiving further includes intercepting a session request that is issued from the service for the legacy LDAP application, wherein the session request includes the alias identity information.

28. The policy and attribute based resource session manager of claim 27 having instructions further comprising managing the session with respect to the service as if the policy based resource session manager were the legacy LDAP application.

29. The policy and attribute based resource session manager of claim 21 wherein the instructions for establishing the session further includes defining the selective resource access policies as at least one of a read operation and a write operation and defining the attributes as selective confidential data related to the principal, wherein

the policies define operations that are permissible on the attributes, and wherein values for the attributes reside in the resource.